Annexure-5

DETECTING DISTRIBUTED DENIAL OF SERVICE ATTACKS ON SOFTWARE DEFINED NETWORKS USING HYBRID APPROACH

SHORT SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna University

by

Gaganjot Kaur
2K17-PFE-003

Under the supervision of

Dr. Prinima Gupta
Associate Professor
Department of Computer Science & Technology
Faculty of Engineering

MANAV RACHNA
Vidyanatanksha

MANAV RACHNA UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING)
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

Year August 2018

MANAV RACHNA
Vidyapatarikhah

MANAV RACHNA UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING)
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

DECLARATION BY THE SCHOLAR

I hereby declare that the short synopsis **"Detecting Distributed Denial of Service Attacks on Software Defined Networks using Hybrid Approach"** being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in department of **Computer Science & Technology** under Faculty of **Engineering** of Manav Rachna University, Faridabad during the academic year 2018.

It is a bona-fide record of original work carried out under the supervision of **Dr. Prinima Gupta** has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that short synopsis is within the plagiarism limit and copy of the same is attached as per University norms.

Gaganjot Kaur
2K17-PFE-003

12/8/2018

Signature of the Supervisor
Full name, Designation and Faculty

Susmita Ray
Chairman, DRC
(FOR PROF. B.M. BEHL)

Proposed Title of Thesis: Detecting Distributed Denial of Service attacks on SDN controller and improvising efficiency of software defined networks using hybrid technique.

Abstract:

Software Defined Network (SDN) is an emerging technology that is used to design, build and manage networks effectively and efficiently. The core functionality of SDN is to take over the control, management and operation of networks in a centralized way by eliminating the problems concerned with distributed network controllers. SDN being future of network has various challenges as well. The various challenges faced by SDN are in terms of its security and interoperability. For example, the main challenge that SDN is to think and work over is the protection of the center controllers from threat and attack. The most popular attack which researchers has thought and worked over is Denial of Service (DOS) attack. Till now, Researchers have proposed and adopted various techniques to protect the controller from DOS attacks. The various techniques existing in literature for evaluating Distributed DOS (DDOS) attacks are Entropy based detection technique, sequential probability ratio test, percentage based detection technique and cumulative based detection technique. The entropy based detection technique are STRIDE, ATTACK and DaMask. The sequential probability technique ratio test is Sphinx. The percentage based detection technique are Openflow, sflow etc and cumulative based detection technique is FRENSCO. All the techniques have been already implemented using data sets of Defense Advanced Research Projects Agency. After implementation it has been analyzed that the sequential probability ratio tests effectively and efficiently to detect the DDOS attacks on the controller and reduces the extent of harming the controller as far as other techniques are concerned. The said techniques are evaluated on certain parameters like threshold value, window size, detection rate and efficiency. The machine learning techniques have been always an effective optimization method in all fields. As the traditional attack detection techniques are generally based on traffic characteristics as well, these various machine learning techniques Naive Bayes, K-Nearest neighbor, K-means and K-medoids are used to arrange the behavior of traffic either normal or abnormal. As per the behavior detection of machine learning technique the optimization technique would help improvise the sequential probability ratio test because it will optimize by reducing the time span of the attack as DDOS attack halts the communication. The basic idea of optimization algorithm is that as per the behavior which is being detected the parameters of optimization algorithm like window size, detection rate and efficiency would be

randomly distributed across the algorithm to eliminate the dispersal of the attack. Classification Technique will definitely give better result in elimination of DDOS attacks and improvising sequential ratio test.

I Introduction

Software defined networks are growing day by day and it is very different and better approach of networking from traditional network. Earlier in the traditional network there has to be a physical device using which all network functionalities are implemented. In today's world where technology is getting advanced both with time and increase of adapting of server virtualization on networks. The challenges faced by traditional network is the reason for emergence of Software Defined Networks. SDN is basically adding programmability to the network. SDN has actually made the traditional network more dynamic, agile that helps the data plane to send the traffic to desired destination by helping the control plane to take certain set of decisions as to where traffic is to be sent. SDN uses the concept of virtualization and the SDN controller is the brain of SDN that helps to take decisions so the entire risk is on the controller itself. The risk is that attackers can manipulate the controller to in turn manipulate the entire network. The attackers can purposefully send purposeless traffic resulting in unauthorized access to enter in the network. SDN controller is more prone to Distributed Denial of Service Attacks so for efficient and effective working of the network it is required to mitigate the DDOS attacks on SDN controller.

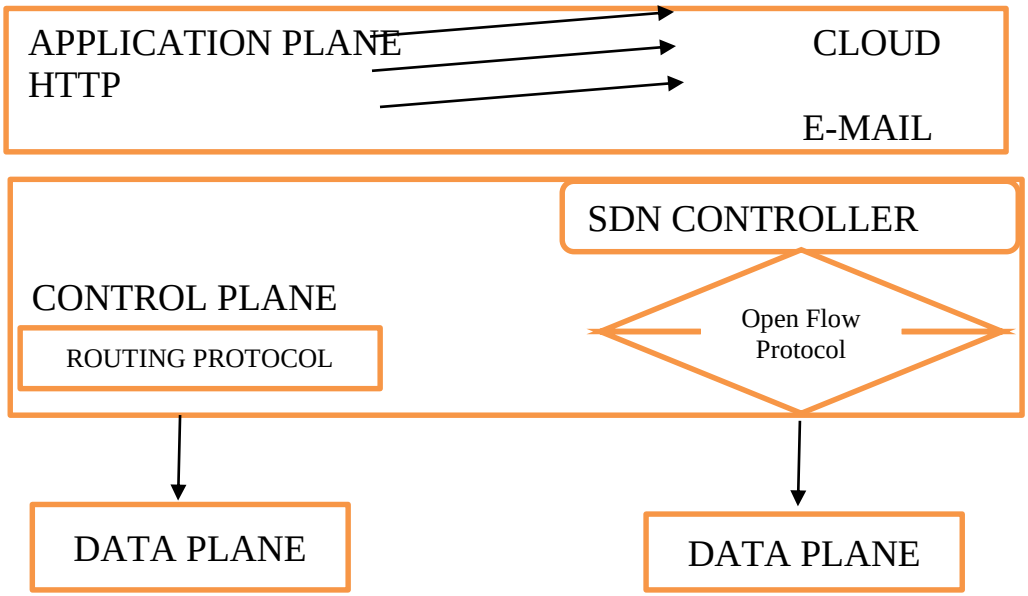


Figure1: Architecture of SDN.

DDOS attacks are basically threats that does not allows its users to make use of network resources or its machines. A machine when is been attacked as a DDOS threat generally gets suspended temporarily or intentionally for its intended users. Many strategies and techniques are been implemented and proposed to avoid DDOS attacks. The main apprehensions of DDOS attacks are the design of networks where in misuse of delivering the packets to a target would result in abnormal behavior of traffic. Overflowing of packets in data plane would result in attack on the controller and forwarding plane. Because of overflow of packets the controller would only process those packets and finally gets exhausted whenever request of new packet comes. This results in loss of SDN Architecture so to avoid this its required to mitigate the DDOS attacks and machine learning techniques are been effectively suggested for mitigation. Machine Learning is a category of applications that normally provides the system to learn and improvise the algorithms to provide accurate results. Different Machine Learning algorithms are been used but they are broadly categorized into supervised and unsupervised learning. In case of supervised learning with the possible outcomes the data is used to train the algorithm that are being characterized. In unsupervised learning neither are any possible outcomes and nor are the trainers to train the specific algorithm. In an unsupervised learning categorization is done on the basis of certain similarities and characteristics of data. Unsupervised learning is classified into two categories of clustering and association. Clustering unsupervised learning is a technique that as per group the algorithms are being classified. Association unsupervised learning is where as per the rules the algorithms are associated. In this, ML classification techniques will classify the threats optimally and convergence time at the controller will be decreased. Machine learning techniques optimizes the solution to make it better than other applied approaches. In our proposed approach machine learning will supposed to maximize the time of detecting the threats in DDOS attacks as the installation in internet or connection to the biggest problems that need to be taken care of.

II Problem Statement

In the earlier methods of detecting threats and evaluating DDOS attacks on SDN controller various techniques used were entropy based detection techniques, sequential probability ratio test, percentage based detection technique and cumulative based detection technique. All the techniques are being implemented using Defense Advanced Research Projects Agency. To

implement these techniques analysis of security on SDN controller is one of the important concern and for that various tools and platforms were being developed and tested. The common used tools for these techniques were STRIDE, FRENSCO, SPHINX and DAMASK. The techniques are being evaluated using certain parameters of Threshold Values, Window size, Detection Rate and Efficiency. Some detection techniques are not certain because of the high threshold values and based on huge traffic on the network. In the proposed method the optimized technique will identify the malicious traffic flow and thus based on the statistics of the flow of packets and the duration it could help reduce the time span of the attacks on the SDN controller.

III. **Review of Literature**

SDN being an emerging approach that is widely preferred to replace standardized networks as it does so by disconnecting the control plane of the network from the underlying hardware like routers, switches etc and connecting the control plane with the data plane using a controller. There is wide research done on the administration of the network. As such there are many challenges in SDN that is to be taken care of like reliability, scalability, interoperability but the major concern of SDN controller is the security of the controller which entirely affects the security of the network as network is universally accessed. As SDN controller is placed centrally so it resolves many issues as well but it is exposed to many threats also. Many researchers have done the research on detecting and mitigating the DDOS attacks on SDN controller. Following is the review of the literature done on the SDN controller and what techniques are been used for detecting and mitigating DDOS attacks on SDN.

OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking 2012 ACM [1], explains about host mutation. In this paper Openflow Random Host Mutation technique is developed that transparently modifies IP address with maximum uncertainty rate. The OF-RHM technique assigns each host a random virtual IP to rephrase to or from real IP of host machine. This technique keeps actual IP address of host machine unchanged. Using OFRHM almost 90% of worms can also be scanned in host machine logistic regression is a specific model for designing of prediction model for categorical data or binary data like 0 or 1. As per author for future scope OFRHM must be implemented considering DDOS and other application layer attacks.

Implementation Challenges for Software-Defined Networks 2013 [2] SDN has become the most prominent network technology having the ability to provide assistance to dynamic nature of the network and its intelligent applications. This paper describes the various challenges faced by SDN in terms of its security, interoperability. The main challenge in SDN is to protect the controllers from threat and attack. To protect the controller from various DOS attacks hybrid approach can be followed of traditional SDN network. As per author for future work the goal is to achieve proper communication of the network and provide secure channel for the transfer of efficient packets and smooth flow of traffic.

Openflow: A security Analysis 2013 IEEE Communications [3] SDN is future of networking. Openflow is one of the widely used standardized protocol in SDN. The paper presents the security aspects concerning openflow protocol. The security analysis is been done using two methods: STRIDE & ATTACK Tree method. This paper discusses the aspect of evaluation, recommendation and analyzing the security part of both the openflow methods. For future recommendations the paper would be helpful to other researchers to design a secure channel while securing the applications of SDN.

Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments 2013 Elsevier [4], SDN is used as it's an emerging technology that decouples the data plane and control plane. The utmost and primarily technique used for SDN architecture is Openflow. The openflow technique adds on different functionality to SDN architecture. This paper presents various components that raises the concern with security attacks to SDN. Packet flow is being monitored using sflow monitoring data. This paper also evaluate the performance of openflow switch on basis of traffic range from low to high.

A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks 2014 IEEE Communications [5], this paper being the survey paper surveys the entire SDN architectural openflow standards discussing the various possibilities for implementation and testing of SDN open interfaces like ForCES and Openflow. The architecture of both the interfaces are discussed in perspective to how implementation is being done of controller and switches. For future reference and research directions new solutions are to be prepared for the challenges to be occurred in SDN of openflow interface.

Comparison of Software Defined Network Implementation Strategies, 2014 Science Direct [6] SDN have become one of the prominent perspective of separating the data plane and control planes. This paper specifies and compares two implementation strategies of SDN. The comparison is done on basis of its features including weakness and strengths and their key feature of working principle. The two strategies are proprietary and Non Proprietary. Depending on the openness of the network both the strategies focuses on the programming concepts. Different vendors provide different strategy of implementations. The key difference between Proprietary and Non Proprietary strategy is that in case of proprietary there is no need to create virtual networks and they can support any workload anywhere but in case of non-proprietary the switches and virtual network overlays help in increasing the high performance. For future reference it is been discussed that as both the strategies have limited approach so one should go with the hybrid approach to work on SDN and increasing the performance.

A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation 2014 IEEE Communications [7] SDN is basically used to dissociate the data and control plane. Normally openflow strategies are preferred. This paper presents the survey of implementation on basis of various characteristics like virtualization, quality of service and language abstraction. This paper has been beneficial for both the academia and industry as it compares the pro and cons of various SDN strategies. For future directions the scope of SDN is widely increasing and to ensure the trustworthy flow preventing from various intrusion and denial of service attacks more research is to be done on the proposed NICE scheme for detection.

Security for Future Software Defined Mobile Networks 2015 International Conference [8] this paper introduces the various security challenges faced by new technologies of SDN, Network flow virtualization and cloud computing. This paper also includes the approach to secure software defined mobile network by taking care of security at various planes to protect both the network users. This paper specifies the summary of security threats in the architecture that has to be taken care of securing communication channels. For the future aspects of this paper the focus is to be done on analyzing the requirements and defining the guidelines for the integration of security components for SDMN architecture.

SD Security: A Software Defined Security Experimental Framework 2015 IEEE ICC Workshop [9] the idea behind SDN as future of network is to separate the two planes. It is the

recent network technology that is taking the market to grow. The main challenge for SDN is its security. This paper addresses the challenge by providing a novel approach of the security mechanism by providing a virtualized environment for SD security systems. The experimental result is implemented on Mininet simulator. The result is evaluated on the basis of three test on Mininet switches. The main focus of these test is to enforce various security attacks on the plane and to evaluate the transfer of packets at certain value. DOS attack detection policies is required to check whether the packets are to be smoothly transferred or are to be dropped. For the future perspective the challenge of security can be extended using developed emulator and it will in turn increase the performance of SDN reducing the overhead.

Securing Software Defined Networks: Taxonomy, Requirements, and Open Issues 2015 IEEE Communication Magazine [10], the existence of SDN is to simplify the networking concepts. Due to high demand of SDN in market the key challenge of SDN to be taken care is its security issues. The article is concerned about the various security solutions for securing SDN. Securing SDN means providing the security on the three layer architecture. Different layers of SDN that is data control and application layer have its own set of responsibility and various researchers have provided an effort to secure the layers. The effort is based on two proposals FortNOX, and FRESCO a security specific application development which is a framework for openflow networks and another one is more towards rule conflicts and authorization. The preferred one is FRESCO as the other one does not much improves the security of application and infrastructure layers as various threats are also being discussed in the paper. For future researchers various open challenges and issues are being discussed in the paper. The paper also provides suggestive measure to follow Openflow technique. By possible discussing various threats and attacks more options gets available for securing SDN.

DDoS attack protection in the era of cloud computing and Software-Defined Networking 2015 Elsevier Computer Journal [11] Cloud Computing and SDN goes hand in hand. This paper addresses one of the important concern of security. Proper defense architecture mechanisms are been designed such to avoid DDOS attacks on the plane. The paper presents an architecture attack defense for DDOS using SDN. The architecture is specified as DaMask and it has two versions of detection i.e DaMask D and M module. Damask as per the network virtualization gets adapted and thus control and configure the mechanism if attacks are there. For future DaMask can be

more configured and worked to evaluate the network performances during the attack defense mechanisms and more appropriate results can be evaluated.

Denial-of-Service Attacks in OpenFlow SDN Networks 2015 IEEE Workshop [12] SDN is a networking model that is thoroughly rebuilding the network plan by isolating the two planes and in SDN mainly the working of controller depends on the behavior of software switches. Because of increasing demand of SDN the threat is also been increasing and SDN have the feature of checking various attacks on the planes. Comparing the traditional network with SDN the attack on traditional network can be protected using various natural defenses while in case of SDN any successful DOS attack can immobilize the complete network. This paper discusses mainly two attacks in SDN both affects the switch as per the flow of packets. The attacks are being out vied on Mininet simulator and certain appliances are being discussed that tempers the results of the attacks. For the future work it is better and worthy to work upon the mitigation strategies that are been discussed in the paper. To prevent an attack it's better to check the limit of packets and as per the rate of flow of packets the traffic on switches can be controlled and for smooth functioning of traffic on the controller. The paper have also given an idea to work on hybrid switches.

SPHINX: Detecting Security Attacks in Software-Defined Networks 2015 NDSS [13], SDN have ability to provide best network with reduced cost and better operational functionalities making sure with more enhanced security for the planes on the network. The authors in the paper list various attacks on the SDN affecting the topology and how can they be rooted on other software switches and hosts. The authors proposed SPHINX mechanism that identifies the known and unknown attacks on the planes and authorizes the flow graph which proximate the sudden updated on the network and accordingly alarms the alert when any doubtful changes occurs on the network. SPHINX mechanism accomplishes the attacks in SDN with low overheads and better performance. For future work proactive attacks are to be detected which normally start up on the controller and thus decreasing the performance. The authors suggest to work more on SPHINX as it have the capability to accurately detect the attacks in the real time and as it produces less overheads also.

Software-Defined Mobile Networks Security 2016 Springer Science Direct [14] Software Defined Network a remarkable technology taking network to higher demand. For increasing the data traffic the concept of network flow virtualization and cloud computing goes hand in hand

with SDN.NFV and cloud computing helps in increasing the flexibility and energy efficiency for software defined networks. This paper presents a survey on software defined mobile networks discussing the concern of security on software defined networks also providing corresponding remedies for the various threats. This paper specifies a STRIDE method that analyses the attacks and threats on software defined networks. Work is done on STRIDE based classification for all data, control and application layers. For future reference the list of security challenges are being listed for mobile defined networks which are to be taken care of.

Enhancing Security in OpenFlow 2016 Capstone Research Project Proposal [15] SDN being an upcoming popularized network have the concern that both the data and control plane are to be taken care of to enhance security. This proposal inspects various threats and flaws in the SDN architecture and present a solution against various security issues in SDN. The authors in the proposal have provided with the novel solution to respond against the network and decreases the overhead. The results in the proposal shows that the architecture which is proposed protects the control channel against various threats.

Detection of Distributed Denial of Service Attacks in Software Defined Networks, 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI) [16] DDOS attack is a major threat that normally occurs on either network layer or application layer. In this paper DDOS attacks are being evaluated according to flow of traffic. Using different machine learning algorithms traffic behavior is analyzed and then algorithms are evaluated on basis of parameters of detection rate and efficiency. For future work DDOS attacks can be implemented using other Machine Learning Algorithms like hidden Markov model.

Defending Cloud Computing Environment against the Challenge of DDoS Attacks Based on Software Defined Network 2017 Springer [17], as technology is increasing day by day the chances to getting attacked are also increasing. Based on the characteristics of SDN it is difficult to detect the vulnerability of the controller on virtual networks so the research is done by the authors to efficiently protect the system from DOS attacks. The authors have proposed an entropy based detection technique to improve the accuracy of detects. The authors have resolved the concern of DDOS attacks without using VM resources. The strategy is specified as entropy based detection that improves detection accuracy as the experiment is based on evaluation of switch under various flow entries.

DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions 2017 Springer Arab J Sci Eng [18], SDN is much preferred by researchers and the most important challenge to be taken care is of DDOS attacks of SDN. Based on characteristics of SDN a survey is being conducted on SDN based DDOS attacks. According to those attacks framework is being designed for the detection and mitigation of DDOS attack for a large scale network considering the formulation to be done for a smart city. Existing DDOS attack techniques have certain pros and cons as according to the threshold value the detection strategies fail to the certain requirement of the application. Prodefense technique can be implemented in any of the programming language and this framework in general works according to the distributed architecture and balances the load as well so detection of attacks becomes easier and faster. For future this work can be implemented carrying more experiments on SDN controller.

FL-GUARD: A Detection and Defense System for DDoS Attack in SDN 2017 ACM. ISBN 978-1-4503-4867 [19] Floodlight guard system is the technique proposed by the authors to detect and prevent the system against DDOS attacks on controller. The authors have used it against dynamic IP address and generate tables accordingly and then block the unwanted traffic on the system. The flood light guard system works only on the spoofing attack on controller ad it can be more effectively used for securing the system from tempering and elevation of privileges threats on the controller for future reference.

Detection of Distributed Denial of Service Attacks using Machine Learning Algorithms in Software Defined Networks 2017 IEEE Journal [20], the controller being more prone to security attacks and is required to detect the attack at earlier stage but less work is done in case of SDN. In this paper the suspicious and malicious attacks are being detected using two Machine learning algorithms - Support Vector Machine (SVM) classifier and the Neural Network (NN) classifier. Results shows it to be effective and for future work it is been suggested to detect attacks using Hidden Markov Model.

Survey on SDN based network intrusion detection system using machine learning approaches 2018 Springer Science Business Media, LLC [21], In this paper the survey is done of Machine learning approaches used to implement SDN based Network Intrusion Detection System. For future reference the challenges that are been discussed of providing greater accuracy and scalability can be achieved using ML/DL techniques for NIDS.

Detection of high rate DDoS attack from flash events using information metrics in software defined networks, 2018 IEEE International Conference [22], in this paper the DDOS attacks are detected by mainly focusing on the openflow information. As DDOS attacks are the main security concern in the SDN so the author suggest to detect the attacks using some metrics like General Entropy and Generalized Information Distance. The metrics values are entirely dependent on the flow of traffic. The detection algorithm is proposed as per the flow of packets and its information is stored in the header field that exists for SDN. The metric values are more appropriate for detecting high rate DDOS attacks. For future work it is predictable that as per the real traffic scenario detections can be made more early and mitigations would be done more easily.

TDDAD: Time-Based Detection and Defense Scheme against DDoS Attack on SDN Controller, 2018 Springer [23], in this author proposes a detection scheme to detect DDOS attacks based on time feature. The very first task for detection is to analyze the behavior of the attack on the network. Pattern recognition of neural network technique is used to recognize the attack and accordingly the action is taken. The result is evaluated taking DARPA data set and the result is then compared with sequential probability ratio test. As a result after comparison it's found that the solution which author have given helps to detect attacks more quickly and accurately.

Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks 2018 IEEE Transactions on Network and Service Management [24], SDN is being widely preferred everywhere and is also used in health care. SDN gives better results in flow of network but the important concern is its security. To detect attacks in SDN the authors have developed a trust based approach based on Bayesian approach that helps to figure out any malicious attacks on health care system. In this paper survey is done from 12 healthcare organizations and considering that attacks depending on various conditions the malicious attacks are being detected. For future work the authors have suggested to improvise the detection technique more quickly and effectively.

A Software-Defined Networking (SDN) Approach to Mitigating DDoS Attacks 2018 Springer [25] DDOS Attacks are being common so many techniques were used to detect and

mitigate DDOS attacks. In this paper traditional approaches to detect and mitigate DDOS attacks are been discussed with its limitations and proposal of extensible productive programmed mitigated solution is been given. For the case study Verizon ISP network is being used for mitigating the attacks and as per the author the study of Verizon ISP network provides the centralized solution to the controller.

Literature Conclusion

In literature survey it has been studied that as such SDN being an emerging paradigm is used and required everywhere but the major concern to be taken care is the security. The important concern is of DDOS attacks and there are various traditional techniques used to detect the attacks. DDOS attacks on the controller brings the entire network at halt and thus it's required to detect and mitigate the threats on the controller. Different methods broadly classified are Sequential Probability Ratio Test, Count based detection method, percentage based detection method and entropy based detection method. DDOS attacks are mainly considered as false IP address to hide the user details. SDN architecture consists of openflow switch that have an entire information about the packets to be received or sent. The attacks are normally on the controller that is an openflow switch. Excess of traffic flow can overload the requests of packet transmission leading to attack on the controller which actually becomes a major concern and is to be solved. DDOS solutions were also being rectified by improving the architecture of the controller making it more scalable and reliable. It was improvised by creating a queue for the incoming packets and congestion of traffic can be controlled using round robin algorithm but it did not work as it became difficult to distinguish the legitimate flow and malicious flow. To resolve the problem another technique used for detecting attacks were described as statistical based solution which was actually storing the value of packet information and the packets that were least required or not that important were being discarded, this method was quite much effective to reduce the congestion but was not able to detect the attack. To detect the attacks preferable method used were entropy based technique and prior to that a hybrid approach of combing open flow and sflow technique was used. In entropy based method certain threshold value was being determined and if the entropy value comes out to be more than the threshold value then attack was being detected. In combination of sflow and openflow technique many combinations were being used that is entropy based technique was also included and on the real time scenario malicious attacks were blocked so it became easier to reduce the overloading of

the controller. The statistical and entropy based techniques were effective but still it takes the time to detect the attacks and then accordingly go for resolving it. Machine learning techniques are also used to detect the DDOS attacks and in that using Support Vector Machine the attacks were detected wherein a model was being designed that sets the points which was used to classify the attack accordingly. In machine learning technique optimizing the flow of traffic on controller will help reduce the time span of attack on controller and thus detecting and mitigating the attack would be faster.

IV Objective of Proposed work

- Conceptual understanding of different type of optimization techniques of machine learning approach to detect and mitigate the DDOS attacks on the controller of SDN.
- Understand the result of statistical entropy based techniques of DDOS attacks and then doing the comparison of the result using optimizing technique of machine learning approach.
- Taking into consideration the timespan of detection of attacks using various statistical techniques and by optimizing the controller using clustering of packets on the network.
- Understand the concept of MATLAB for SDN as a research tool for analyzing of packets, detection of attacks, and timespan during the detection.

V Methodology

Methodology of Clustered Optimization Technique which involves quantitative research method which involves modeling and analyzing data sets taking into consideration the number of packets to be sent and received on a network and giving the certain threshold value to detect the malicious flow of packets.

STEP1: Collection of data is done from online repository (UCI Repository).

Characteristics of data set

Data type: time series data set

Attribute characteristics: Real

Associated task: Traffic Flow

Source: UCI repository

STEP2: Flow of traffic is an observation that tells which the legitimate flow is and which is malicious flow on the network in a sample data of the packets. It means that, the analyst decide what should be considered and should not be considered. Before unusual observations could be selected out, it is mandatory to find the feature of normal observations.

STEP3: MATLAB tool will be used as a framework where in the data set of packets would be developed by creating a virtual network with various hosts, links and switches on a machine. The packets would be transmitted and the rate in which packets are being transmitted or received would be checked.

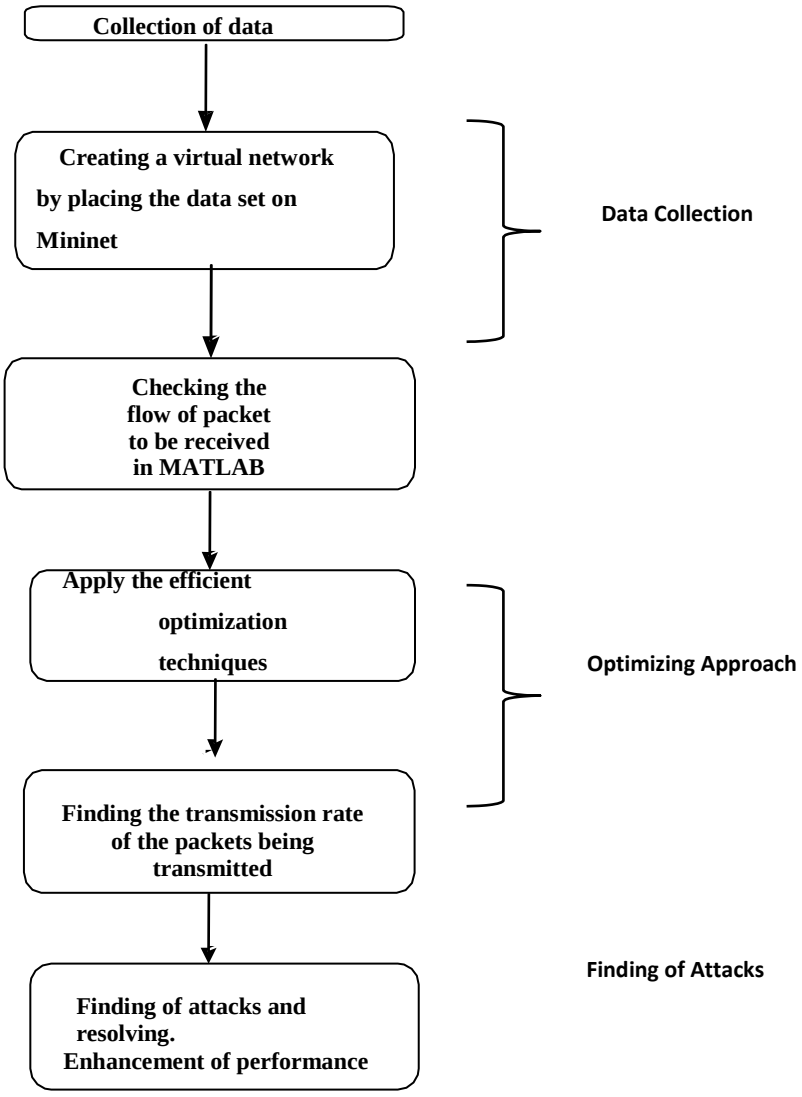

Collection of data
Creating a virtual network by placing the data set on Mininet
Data Collection
Checking the flow of packet to be received in MATLAB
Apply the efficient optimization techniques
Optimizing Approach
Finding the transmission rate of the packets being transmitted
Finding of Attacks
Finding of attacks and resolving. Enhancement of performance

Figure2: Methodology of detection

STEP 4: Calculation of transmission rate. Rate at which packets are being sent will be checked and calculated that will help detect malicious flow.

STEP 5: Depending on flow of traffic detect the various attacks using dataset in SDN.

STEP 6: After detecting the attack apply optimizing technique and resolve the attack.

STEP 7: During Detection of attack the result would be later on compared using entropy based technique. Optimizing would result in reducing the time span of attack and help in resolving the attack faster and giving better performance.

References

[1] Jafar Haadi Jafarian, Ehab Al-Shaer, Qi Duan, OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking HotSDN'12, August 13, 2012, Helsinki, Finland. Copyright 2012 ACM 978-1-4503-1477-0/12/08.

[2] Sakir Sezer, Sandra Scott-Hayward, and Pushpinder Kaur Chouhan, Implementation Challenges for Software-Defined Networks, IEEE Communications Magazine July 2013 0163-6804/13/$25.00 © 2013 IEEE.

[3] Rowan Kl¨oti, Vasileios Kotronis, Paul Smith, OpenFlow: A Security Analysis, 978-1-4799-1270-4/13/$31.00 c 2013 IEEE.

[4] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, V. Maglaris, Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments, 2013 Elsevier Science Direct Computer Networks, journal homepage: www.elsevier.com/locate/comnet

[5] Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 3, THIRD QUARTER 2014.

[6] Muhammad H. Razaa,∗, Shyamala C. Sivakumarb, Ali Nafarieha, Bill Robertsona, A Comparison of Software Defined Network (SDN) Implementation Strategies, 2nd International Workshop on Survivable and Robust Optical Networks (IWSRON), Science Direct, Elsevier.

[7] Fei Hu, Qi Hao, and Ke Bao, A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2014.

[8] Madhusanka Liyanage∗, Ijaz Ahmad, Mika Ylianttila, Jesus Llorente Santos, Raimo Kantola, Oscar Lopez Perez, Mikel Uriarte Itzazelaia, Edgardo Montes de Oca, Asier Valtierra, Carlos Jimenez, Security for Future Software Defined Mobile Networks, 978-1-4799-8660-6/15 $31.00 © 2015 IEEE, DOI 10.1109/NGMAST.2015.43.

[9] Ala' Darabseh1, Mahmoud Al-Ayyoub1, Yaser Jararweh1, Elhadj Benkhelifa2, Mladen Vouk3, and Andy Rindos4, SDSecurity: A Software Defined Security Experimental Framework, IEEE ICC 2015 - Workshop on Cloud Computing Systems, Networks, and Applications (CCSNA).

[10] Adnan Akhunzada, Ejaz Ahmed, Abdullah Gani, Muhammad Khurram Khan, Muhammad Imran, and Sghaier Guizani, Securing Software Defined Networks: Taxonomy, Requirements, and Open Issues, IEEE Communications Magazine • April 2015, 0163-6804/15/$25.00 © 2015 IEEE.

[11] Bing Wang ⇑, Yao Zheng, Wenjing Lou, Y. Thomas Hou, DDoS attack protection in the era of cloud computing and Software-Defined Networking, 2015 Elsevier Computer Networks, journal homepage: www.elsevier.com/locate/comnet.

[12] Rajat Kandoi, Markku Antikainen, Denial-of-Service Attacks in OpenFlow SDN Networks, 978-3-901882-76-0 @2015 IFIP

[13] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, Vijay Mann, SPHINX: Detecting Security Attacks in Software-Defined Networks, NDSS '15, 8-11 February 2015, San Diego, CA, USA Copyright 2015 Internet Society, ISBN.

[14] Min Chen1 · Yongfeng Qian1 · Shiwen Mao2 · Wan Tang3 Ximin Yang3, Software-Defined Mobile Networks Security, Mobile Netw Appl (2016) Mobile Netw Appl (2016) Springer Science+Business Media New York 2016

[15] Niketa Chellani, Prateek Tejpal, Prashant Hari, Vishal Neeralike , Enhancing Security in OpenFlow, Capstone Research Project Proposal, April 22, 2016.

[16] Lohit Barki, Amrit Shidling, Nisharani Meti, Narayan D G and Mohammed Moin Mulla, Detection of Distributed Denial of Service Attacks in Software Defined Networks, 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India.

[17] Shuen-Chih Tsai, I-Hsien Liu, Chien-Tung Lu, Chan-Hua Chang, and Jung-Shian Li, Defending Cloud Computing Environment Against the Challenge of DDoS Attacks Based on Software Defined Network, © Springer International Publishing AG 2017, J.-S. Pan et al. (eds.), Advances in Intelligent Information Hiding and Multimedia, Signal Processing, Smart Innovation, Systems and Technologies 63, DOI 10.1007/978-3-319-50209-0_35.

[18] Narmeen Zakaria Bawany1 · Jawwad A. Shamsi1 · Khaled Salah2, DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions, 2 February 2017 Springer Arab J Sci Eng (2017) 42:425–441.

[19] Jing Liu, Yingxu Lai, Nisharani Meti, Shixuan Zhang, FL-GUARD: A Detection and Defense System for DDoS Attack in SDN, ICCSP '17, March 17-19, 2017, Wuhan, China, © 2017 ACM. ISBN 978-1-4503-4867-6/17/03…$15.00, DOI: http://dx.doi.org/10.1145/3058060.30580745

[20] Nisharani Meti1, Narayan D G2 and V. P. Baligar 3, Detection of Distributed Denial of Service Attacks using Machine Learning Algorithms in Software Defined Networks, 978-1-5090-6367-3/17/$31.00 ©2017 IEEE

[21] Narmeen Zakaria Bawany1 · Jawwad A. Shamsi1 · Khaled Salah2, Survey on SDN based network intrusion detection system using machine learning approaches, Peer-to-Peer Networking and Applications https://doi.org/10.1007/s12083-017-0630-0, # Springer Science+Business Media, LLC, part of Springer Nature 2018.

[22] Kshira Sagar Sahoo*, Mayank Tiwary† , Bibhudatta Sahoo∗, Detection of High Rate DDoS Attack From Flash Events Using Information Metrics in Software Defined Networks 2018, 10th International Conference on Communication Systems & Networks (COMSNETS).

[23] Jie Cui1,2, Jiantao He1,2, Yan Xu1,2, and Hong Zhong1,2, TDDAD: Time-Based Detection and Defense Scheme Against DDoS Attack on SDN Controller Australasian Conference on Information Security and Privacy ACISP 2018: Information Security and Privacy pp 649-665. Published in Elsevier.

[24] Weizhi Meng, Member, IEEE, Kim-Kwang Raymond Choo, Senior Member, IEEE, Steven Furnell, Athanasios V. Vasilakos, and Christian W. Probst, Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. IEEE Transactions on Network and Service Management (Volume: 15, Issue: 2, June 2018).

[25] Hubert D'Cruze, Ping Wang, Raed Omar Sbeit, Andrew Ray, A Software-Defined Networking (SDN) Approach to Mitigating DDoS Attacks, Published in July 2018, Advances in Intelligent Systems and Computing, DOI: 10.1007/978-3-319-54978-1_19.

[26] Basheer Husham Ali Al-Mafrachi ,Thesis B.Sc., Al-Mustansiriya University, 2010 Detection Of Ddos Attacks Against The Sdn Controller Using Statistical Approaches.

MANAV RACHNA
Vidyanatariksha

Swami Vivekananda Library and Resource Centre
Manav Rachna University

SIMILARITY VERIFICATION CERTIFICATE

Title: DETECTING DISTRIBUTED DENIAL OF SERVICE ATTACKS IN SOFTWARE DEFINED NETWORKS USING HYBRID APPROACH

Researcher : GAGANJOT KAUR

Registration Number:

Supervisor: Dr. PRINIMA GUPTA

Department: COMPUTER SCIENCE & TECHNOLOGY

This is to certify that the above mentioned Short Synopsis / ~~Thesis~~ was scanned for similarity index through Turnitin Software on 12-Aug-2018 with submission ID 989253298 and the similarity index was found to be 7%. The complete report running into 22 Pages, 6234 Word count with File Size 4625 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

Swami Vivekananda Library and Resource Centre Faridabad * Manav Rachna University * 12/8/2018

Date: 12-Aug-2018

The complete report of the above Short Synopsis/ ~~Thesis~~ has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/ ~~Thesis~~ may be considered for further processing.

12/8/2018
Research Scholar

12/8/2018
Research Supervisor

GAGANJOT_Synopsis_SDN12.8.2018.

by Gaganjot Kaur

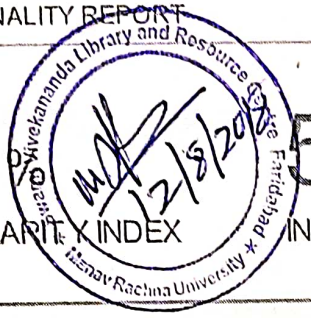
Submission date: 12-Aug-2018 09:41AM (UTC+0530)
Submission ID: 989253298
File name: GAGANJOT_Synopsis_SDN.doc (155.5K)
Word count: 6234
Character count: 35197

short

GAGANJOT_Synopsis_SDN12.8.2018.

ORIGINALITY REPORT

Excluding matches less than 14 words



7%	5%	6%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Lohit Barki, Amrit Shidling, Nisharani Meti, D G Narayan, Mohammed Moin Mulla. "Detection of distributed denial of service attacks in software defined networks", 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016 Publication	1%
2	hrcak.srce.hr Internet Source	1%
3	Submitted to Wright State University Student Paper	<1%
4	Nisharani Meti, D G Narayan, V. P. Baligar. "Detection of distributed denial of service attacks using machine learning algorithms in software defined networks", 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017 Publication	<1%

5	research.aalto.fi Internet Source	<1%
6	www.mdpi.com Internet Source	<1%
7	Submitted to Staffordshire University Student Paper	<1%
8	mru.edu.in Internet Source	<1%
9	business.utsa.edu Internet Source	<1%
10	Submitted to Northcentral Student Paper	<1%
11	Nasrin Sultana, Naveen Chilamkurti, Wei Peng, Rabei Alhadad. "Survey on SDN based network intrusion detection system using machine learning approaches", Peer-to-Peer Networking and Applications, 2018 Publication	<1%
12	www.djece.org Internet Source	<1%
13	dl.acm.org Internet Source	<1%
14	dblp.uni-trier.de Internet Source	<1%

15	digital-library.theiet.org Internet Source	<1%
16	www.cloudbus.org Internet Source	<1%
17	mnm-team.org Internet Source	<1%
18	Madhusanka Liyanage, Ijaz Ahmed, Mika Ylianttila, Jesus Llorente Santos et al. "Security for Future Software Defined Mobile Networks", 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015 Publication	<1%
19	onlinelibrary.wiley.com Internet Source	<1%
20	www.cnsm-conf.org Internet Source	<1%

Exclude quotes	On	Exclude matches	< 14 words
Exclude bibliography	On		